个人云存储服务的技术安全风险关键影响因素识别与分析*

■ 程慧平[1,2] 彭琦[1]
[1] 湖北工业大学经济与管理学院 武汉 430068 [2] 西北大学公共管理学院 西安 710127

摘要:[目的/意义]近年来个人云存储服务的技术安全问题屡见不鲜,严重影响了个人云存储服务用户持续使用率。识别和分析使用云存储服务的技术安全风险的关键影响因素,对于个人云存储服务提供商提供安全云存储服务、提高个人云存储服务用户粘性具有重要实践意义。[方法/过程]基于文献调研、专家访谈、云计算安全报告(Gartner)、云计算安全架构与标准(ENISA、CSA、FedRAMP、MTCS),构建个人云存储服务的技术安全风险影响因素指标体系。通过专家问卷调查得出个人云存储服务的技术安全风险评估体系中各影响因素之间的直接影响矩阵,运用 Fuzzy-DEMATEL 方法对个人云存储服务技术安全风险影响因素的因果关系及重要程度进行分析,揭示个人云存储服务技术安全风险关键影响因素。[结果/结论]个人云存储服务技术安全风险关键影响因素包括:访问控制、服务/账户劫持、软件安全风险、虚拟化漏洞、数据传输安全。最后,依据实证研究结论,为个人云存储服务提供商构建安全云存储服务提供可行的技术建议。本研究丰富了个人云存储服务安全风险理论研究成果,为个人云存储服务提供商保障用户数据安全提供实践参考。

关键词:个人云存储服务 云存储安全 云计算安全 Fuzzy-DEMATEL 技术安全风险
分类号:G250
DOI:10.13266/j.issn.0252-3116.2019.16.005

1 引言

互联网、社交媒体及移动终端设备的快速发展给人们的社会生活带来了极大的便利,也使得用户个人信息数据呈指数性增长,激发了人们对数据高效存储的迫切要求。个人云存储服务的利用成为解决这一问题的有效途径。个人云存储以其高效、便捷、成本低等优势吸引了越来越多网民的关注。个人用户可按需购买存储服务,相较于传统的存储方式更节约存储资源,且降低了用户自身存储和计算资源有限所带来的诸多约束。个人云存储融合了面向服务构架(SOA)、Web 2.0 技术和虚拟化等多种技术,但在其发展过程由于技术的不成熟带来的安全风险已经直接影响到个人云存储系统的正常运作,导致个人云存储服务提供商信誉大大降低[1]。近几年,由于技术漏洞导致云端数据泄露现象屡见不鲜,本文整理近年来国外发生的大量云服务安全事件,见表1。

艾媒咨询发布的《2016 年中国个人云盘行业研究报告》显示,2016 年中国个人云存储用户规模直线下降至 3.96 亿人,仅有 7.3% 的用户持续使用云盘,导致这一现象的主要原因是用户对个人云存储服务提供商的安全保障能力及风险控制能力的不信任[2]。随着云计算安全风险事件频发,以及基于网络应用的个人云存储用户转移门槛低,用户持续使用不足,使个人云存储服务发展面临困境。如何在保障个人云存储服务技术安全的前提下,促进用户持续使用是保证个人云存储市场可持续发展的根本之道。因此,技术安全是个人云存储服务实践发展过程中亟待解决的关键问题。

本研究主要实现以下两个目标:①从技术安全层面识别个人云存储服务安全风险因素,构建个人云存储服务的技术安全风险评估指标体系;②揭示个人云存储服务的技术安全风险复杂系统中因素之间的因果关系,并确定个人云存储技术安全风险关键影响因素。

* 本文系国家自然科学基金青年项目"面向个人用户的云存储服务使用行为机理及安全风险控制研究"(项目编号:71603075)研究成果之一。
作者简介:程慧平(ORCID:0000-0003-4631-7997),教授,博士,E-mail:chenghuiping@nwu.edu.cn;彭琦(ORCID:0000-0001-5628-3482),硕士研究生。
收稿日期:2018-10-30 修回日期:2019-02-21 本文起止页码:43-53 本文责任编辑:王传清

表 1 近年来云服务安全事件

时间	服务提供商	事件描述
2009 年 3 月	谷歌	谷歌邮箱爆发长达 4 个小时全球性故障
	微软	微软云计算平台 Azure 骤停约 22 小时
2009 年 6 月	Rackspace	云服务中断致使业务脱机 15 到 20 分钟
2010 年 9 月	谷歌	谷歌邮箱再次爆发大规模的用户数据泄漏事件,高达 15 万用户受到影响
2011 年 4 月	亚马逊	亚马逊公司爆出了史前最大的云计算数据中心宕机事件
2012 年 2 月	微软	云计算平台 Azure 所有集群的服务管理功能都被禁用
2013 年 8 月	亚马逊	亚马逊 AWS 云服务宕机,对 Amazon. com 主页和 AWS 造成了严重影响
2014 年 9 月	苹果	黑客对 iCloud 账户密码进行破解,导致多位好莱坞女明星的不雅照片曝光
2016 年 3 月	Salesforce	欧洲的一些客户不得不面对由于存储问题导致长达 10 小时的 CRM 故障
2016 年 4 月	谷歌	Cloud Platform 出现 18 分钟的中断
2016 年 6 月	苹果	Apple 云发生广泛的服务中断,包括零售服务、备份服务、App Store 服务等
2016 年 9 月	微软	微软 Azure 服务在波及所有地区用户的全球性 DNS 故障中发生降级
2017 年 3 月	谷歌	云服务商 Cloudflare 的流量泄漏漏洞,超过 550 万网站的上亿用户受到影响

2 文献综述

当前已有的云计算安全研究主要分为两个部分:

(1)云计算安全风险因素构成和评估研究。云计算安全问题已得到学术界众多学者的关注,已有文献研究主要集中在以下 3 个方面:第一,云计算安全风险构成研究:欧洲网络信息安全局(ENISA)[3]从政策和组织风险、技术风险、法律风险以及不特定云风险 4 个角度共提出了 35 个风险因素。D. Zissis 等[4]从应用层、虚拟层、物理层提出目前云计算面临的 28 个威胁以及 18 个安全要求。A. Singh 等[5]从数据存储与计算安全、虚拟化安全、因特网和与服务有关安全、网络安全、访问控制、软件安全、信任管理、合规和法律 8 个方面构建了云计算安全指标体系。第二,从理论上提炼云计算安全主要风险因素:早在 2008 年 Gartner[6]发布的《云计算安全风险评估》研究报告中就提出了云计算的七大风险。云安全联盟(CSA)[7]列出了 2016 年"十二大云安全威胁"。N. Khan 等[8]和 G. Ramachandra 等[9]提出了云计算的 12 个威胁和漏洞,并且其中有多个影响因素与 CSA2016 年发布的"云安全"威胁一致,分别是:服务/账户劫持、共享技术风险、不安全的 APIs、恶意内部人士、数据泄露和拒绝服务攻击。上述研究主要是对云计算安全风险因素简单的定性讨论。第三,云计算安全风险评估方法:A. Shameli-Sendi 等[10]提出了一种云计算安全风险评估框架并以某工业汽车公司为例进行了实证研究。J. Liu 等[11]提出了一种基于模糊熵权的风险评估方法。G. T. R. Lin 等[12]构建了云计算中信息安全管理的关键成功因素层次模型,并应用模糊层次分析法进行了实证分析。F. Lin 等[13]提出了一种基于云重心理论的云计算系统风险评估方法,通过模拟实验验证了其可行性。

(2)云计算安全标准和安全控制体系研究。云计算安全问题引起各国政府和云计算标准组织高度关注,已有了较多安全标准、控制体系及指南。ISO/IEC 27017 国际云保障标准为云服务提供商提供了安全云存储的发展方向,可作为云服务提供商接受保护控制的标杆性文件,且提出了相关控制模式以解决云安全威胁和风险[14-15]。联邦风险和授权管理计划(FedRAMP)旨在为联邦机构提供云计算服务,监管和授权提供标准化的方法,与 ISO/IEC 相较而言,FedRAMP 更侧重于云计算安全维护方面[16]。多层云安全(MTCS)新加坡标准(SS584)旨在明确云服务提供商的安全要求,并且能够满足不同用户对隐私数据和关键性业务的安全要求,该标准主要关注云服务的可用性[17]。CSA[18]发布的《云计算关键领域安全指南》提出了 13 个云计算的关键安全领域,为云服务提供商和用户识别风险提供参考。ENISA 发布的《云计算合同安全服务水平监测指南》从服务等级协议(SLA)角度为云服务商的服务合规操作提供指导[19]。

综上所述,现有针对云计算安全相关研究以理论探讨为主,而实证分析研究有待加强。已有的云计算安全风险研究中针对个人云存储安全风险影响因素的研究较少,尤其缺少从技术安全维度的定量研究,揭示个人云存储安全风险因素之间相互关系的研究更为鲜见。本文通过识别影响个人云存储服务的技术安全风险因素,分析各影响因素之间的相互关系及相对重要程度,找出关键技术安全风险因素,以期为个人云存储服务安全风险管理决策的利益相关者提供理论依据。

3 个人云存储服务技术安全风险指标体系构建

个人云存储是涵盖云计算分布式存储以及高效共享等特点的新兴在线存储系统，因此个人云存储服务技术安全风险既包括了传统存储信息技术安全风险，又蕴含分布式存储和共享技术等带来的云特有技术安全风险[6,20]。本研究通过文献调研、专家访谈、云计算安全报告(Gartner)、云计算安全架构与标准(ENISA、CSA、FedRAMP、MTCS)，构建个人云存储服务技术安全风险影响因素指标体系(见表2)，从传统技术安全风险和云特有技术安全风险两者整合的视角，构建个人云存储服务技术安全风险指标体系(见图1)。

表2 个人云存储服务技术安全风险指标体系及来源

二级指标	三级指标	指标题项或解释	指标来源
传统技术安全风险	F1 访问控制	1、用户认证	A. Singh[5](2017),FedRAMP(2015)[16]
		2、授权(恶意内部人员)	ENISA(2009)[3],CSA(2016)[7]
	F2 服务/账户劫持	黑客盗取用户身份凭证，从而访问云的关键区域，损害服务的安全性	CSA(2016)[7]
	F3 资源耗尽	资源消耗未得到控制	ENISA(2009)[3]
	F4 数据完整性风险	1、数据丢失和泄露	CSA(2016)[7],M. H. Shirvani(2018)[21]
		2、数据篡改和破坏	D. Zissis(2012)[4],M. Mackay(2012)[22]
	F5 加密及密钥管理	1、数据加密技术	MTCS(2016)[17],W. M. Kang(2015)[23]
		2、密钥管理技术	FedRAMP(2015)[16],ENISA(2009)[3]
	F6 网络安全风险	1、网络带宽	A. Singh(2017)[5]
		2、恶意代码/软件攻击	M. Walterbush(2017)[24]
	F7 硬件安全风险	硬件设备丢失或遭到破坏导致用户数据丢失或泄露风险	姜茸(2016)[25],L. Coppolino(2016)[26]
	F8 数据备份和恢复	云服务商能够按时备份用户数据，并在需要时快速地恢复用户数据	M. Choi(2015)[27],S. Singh(2016)[28]
	F9 服务器引擎漏洞	服务器引擎代码可能存在漏洞，容易受到攻击或意外故障	ENISA(2009)[3]
	F10 软件安全风险	1、软件更新与升级隐患	姜茸(2016)[25]
		2、不安全的接口和APIs	A. Singh(2017)[5],CSA(2016)[7]
		3、软件自身漏洞	阮树骅(2018)[29]
云特有技术风险	F11 虚拟化漏洞	1、虚拟机映像管理漏洞	D. Zissis(2012)[4],A. Singh(2017)[5]
		2、虚拟机监视器漏洞	K. Hashizume (2013)[1], M. H. Shirvani (2018)[21]
		3、虚拟机克隆漏洞	A. Singh(2017)[5]
		4、虚拟机之间的漏洞	A. Singh(2017)[5],M. H. Shirvani (2018)[21]
		5、拒绝服务攻击	ENISA(2009)[3],CSA(2016)[7]
		6、数据隔离	ENISA(2009)[3],Gartner(2008)[6]
	F12 数据移植	数据移植技术不够完善，可能会导致用户数据在迁移过程中丢失	M. Choi(2015)[27],C. Rong(2013)[30]
	F13 数据传输安全	传输过程中存在嗅探、欺骗、中间人攻击、侧信道攻击等风险	ENISA(2009)[3],N. Brender(2013)[31]
	F14 数据删除	数据的不彻底删除可能会导致用户数据泄露	ENISA(2009)[3],A. Singh(2017)[5]

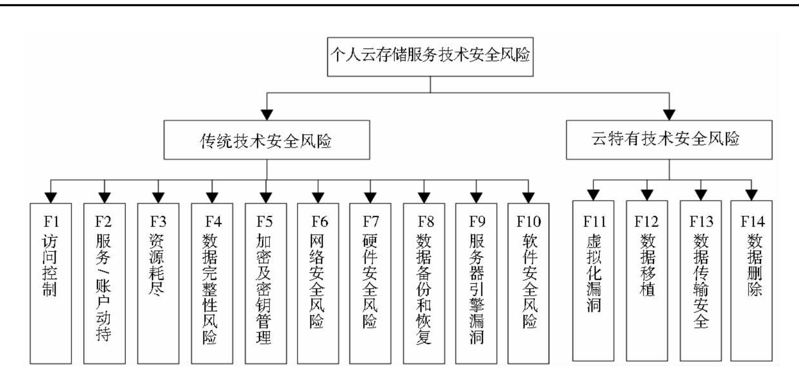


图1 个人云存储服务技术安全风险指标体系

3.1 传统技术安全风险

(1)访问控制主要包括身份认证和授权。身份认证也称身份鉴别,是对访问个人云存储系统的用户身份信息进行确认。个人云存储系统面向庞大的用户群,每个用户都有唯一的身份信息,系统需要通过健全的身份认证技术对用户的身份信息进行确认。其次,每个云存储用户可能在不同的云存储平台上进行注册,且习惯使用相同的账号和密码,这种情况则更要求个人云存储服务提供商提供更加强大的用户身份认证技术。授权是指对用户或应用程序的权限授予或拒绝的过程,恶意授权用户或应用程序可以访问被禁止的资源并执行非法数据操纵。值得特别注意的是个人云存储服务提供商内部人员权限的限定,恶意的内部人员可能会违反职业道德滥用权限非法访问用户数据,从而导致用户隐私泄露。

(2)服务/账户劫持是指攻击者盗取授权用户登录凭证,非法访问云中关键位置,窃听用户活动任务、进行不正当的数据交易、操纵等,并且使得用户无法正常登录。服务/账户劫持可以通过欺诈、网络钓鱼和软件漏洞来实现。

(3)资源耗尽是指资源消耗未得到有效控制而超出计划使用量。云存储服务资源在分配时存在一定的计算风险,包括配置资源使用的不准确模型、公共资源分配算法容易受到公平性的影响、资源配置不足3种风险,将导致服务中断和个人云存储服务提供商声誉受损。这种风险也可能是由拒绝服务攻击所导致。

(4)数据完整性风险是指用户存储在云端数据的完整性,主要包括数据丢失和泄露、数据篡改和破坏两个方面。数据丢失和泄露是指数据被非法删除、变更和盗窃,并且原始数据没有进行备份。数据丢失和泄露的主要原因是缺乏成熟的认证、授权及备份容灾技术。数据篡改和破坏是指攻击者对用户数据的修改、破坏数据结构等。数据的丢失和泄露、数据篡改和破坏都会导致用户数据失去完整性,从而使得用户对个人云存储服务提供商失去信心以致于不再将数据存放在云端。

(5)加密及密钥管理主要包括数据加密技术和密钥管理技术。个人云存储服务提供商采用的数据加密技术不成熟,攻击者可以对数据直接解密,导致用户数据泄露;另外,数据加密技术本身存在的漏洞可能造成数据结构的破坏从而导致数据失效、数据损坏等情况。用于加密、身份验证或数字签名的加密密钥丢失或损坏可能导致数据丢失或拒绝服务等。

(6)网络安全风险主要包括网络带宽和网络恶意代码/网络恶意软件注入两个方面。网络带宽直接影响云服务的性能,高速稳定的网络才能支持众多用户并发操作时不发生网络中断、网络延迟等问题。目前,云端数据安全的很多危机都来自于网络攻击,对此,个人云存储服务提供商采取了网络监控防范措施,但目前该技术仍不够完善,并不能监控到所有可能的网络攻击。

(7)硬件安全风险主要是指存储硬件设备损坏带来的风险。由于设备监控技术和设备保护技术的不完善,当硬件受到不可抗力的自然灾害或人为破坏时造成数据丢失或泄露风险。

(8)数据备份和恢复是指个人云存储服务提供商能够按时备份用户数据,并在需要时及时、快速地恢复用户数据,从而降低因设备故障原因造成的数据丢失或不可用等风险。

(9)服务器引擎漏洞是指服务器引擎代码可能存在漏洞,容易受到攻击或意外故障,非法用户通过攻击服务器引擎,能够越过用户之间的虚拟隔离,从而获取其他用户的数据访问权限,进行不正当的数据操作。

(10)软件安全风险主要包括软件更新与升级隐患、不安全的接口和APIs、软件自身漏洞3个方面。移动终端系统都会面临更新换代,每次更新过程中都可能出现各种不同的问题。用户要实现与云平台的交互,必须依赖于个人云存储服务提供商提供的软件接口或APIs才能进行相应的数据操作。这些接口一旦出现漏洞而被攻击者所利用,将导致云服务无法正常提供。软件自身含有漏洞将使得攻击者有可乘之机,可轻松越过系统防护进行攻击。

3.2 云特有技术安全风险

(1)虚拟化漏洞。虚拟化技术是实现云计算的核心技术,只有通过虚拟化技术,云计算才能实现按需存储的功能,但是虚拟化技术的出现也给个人云存储带来了新的技术安全风险——虚拟化漏洞。虚拟化漏洞主要包括虚拟机映像管理漏洞、虚拟机监视器漏洞、虚拟机克隆漏洞、虚拟机之间的漏洞、拒绝服务攻击、数据隔离6个方面。云的动态性允许用户创建新的虚拟机映像或使用以前创建的映像,该功能可能会导致恶意用户创建含有恶意软件的映像或者找到映像代码中可能的攻击点进行攻击;另一方面,恶意虚拟机映像不正当观察用户活动或数据会导致用户信息泄露。虚拟机监视器内部结构的复杂性和多接入点特性可能会带来大量携带病毒的媒介攻击;其次,由于虚拟机监视器

的透明性,可能会引起 Rootkit 攻击。恶意用户可通过控制虚拟机监视器监视其他虚拟机的活动从而窥探用户的数据信息。虚拟机克隆是将虚拟机移动到其他服务器的过程,多个正在运行的虚拟机同时复制相同的映像,复制过程可能会导致包含用户私密密钥和其他隐私的映像泄漏到其他的虚拟机中。虚拟机的可复制性虽然为个人云存储快速发展提供了条件,但是复制过程中带来的风险是不可忽视的。虚拟机之间的漏洞是指虚拟机群中各虚拟机之间的相互攻击,包括跨虚拟机攻击、虚拟机跳跃攻击(攻击者基于一台虚拟机窃取同一虚拟机监视器上的其他虚拟机的访问权限进行攻击)、重复攻击及侧信道攻击等。拒绝服务攻击是指攻击者通过控制单个虚拟机耗尽了所有的资源,导致其他虚拟机由于资源匮乏而无法正常工作,从而拒绝用户的正常服务请求。个人云存储多租户模式使得不同用户之间的数据隔离措施尤为重要。虚拟机之间虽然逻辑上是相互独立的,但实际上所有的虚拟机仍是共享相同的资源池,有可能导致虚拟机之间相互攻击,引发数据泄露现象。

(2)数据移植技术是个人云存储系统长期稳定运作的重要保证。由于云存储分布式存储的特点,云端数据在不同的 SaaS 平台之间迁移过程中可能因为数据导入导出格式不兼容而导致数据丢失;另外,在迁移过程中可能会发生服务中断、黑客攻击等导致数据丢失或泄露。

(3)由于分布式系统和共享技术的特点,云存储数据传输技术相较于传统的存储技术具有更多的数据传输途径,因此带来了更多不可控的风险。数据传输过程中可能存在嗅探、欺骗、中间人攻击、侧信道攻击等风险。

(4)数据删除不彻底可能会导致用户数据泄露。云端数据可能会在多处位置进行备份存储,用户发送删除指令,但个人云存储服务商可能没有将所有的备份数据彻底删除或是个人云存储服务提供商违反职业道德并没有执行删除操作,而将用户数据进行交易处理导致用户数据泄露。

4 Fuzzy-DEMATEL 方法

决策试验与评价实验室(DEMATEL)方法主要用于分析复杂系统各因素之间互相影响程度。以图论为基础,构建系统因素之间的可视化因果图,以便于更好地理解系统元素之间的关系,从而得到高效的解决方案[32]。由于现实问题的不确定性,专家在评分时多使用"重要""比较重要"等模糊的语义表达。为降低 DEMATEL 方法的主观性和模糊性,综合模糊理论和 DEMATEL 方法进行计算分析。Fuzzy-DEMATEL 方法的计算步骤如下。

步骤 1:确定研究问题所包含的一组影响因素 F = {F1,F2,……,Fn},设计专家评估语义量表,将因素之间的影响程度强弱分为 5 个等级,具体影响程度等级见表 3。

步骤 2:邀请专家在理解语义量表的基础上,对因素之间的影响程度打分,得到一个原始直接影响矩阵 A,矩阵 A 是一个非负矩阵且主对角线为 0,其中 a_{ij} 表示元素 F_i 对元素 F_j 的影响程度。

步骤 3:利用三角模糊数对原始直接影响矩阵 A 进行模糊化处理,并利用 S. Opricovic[33] 开发的将模糊数据转换为清晰值的方法(CFCS)进行去模糊化处理得到清晰直接影响矩阵 Z。

利用三角模糊数的隶属函数公式(见公式(1)),计算出合适的三角模糊数 $N=(l,m,r)$,其中 l 表示作用强度的保守值,m 表示该作用强度的可能值,r 表示该作用强度的乐观值,得出语意转化表(见表 3)。

$$\mu_N(x)=\begin{cases}0, & x<l\\ \dfrac{x-l}{m-l}, & l\leqslant x<m\\ \dfrac{r-x}{r-m}, & m\leqslant x\leqslant r\\ 0, & x>r\end{cases} \quad \text{公式(1)}$$

表 3 语意转化情况

影响等级语意变量	对应的分值	对应的三角模糊数
没有影响(N)	0	(0,0,0.25)
非常弱影响(VL)	1	(0,0.25,0.5)
弱影响(L)	2	(0.25,0.5,0.75)
强影响(H)	3	(0.5,0.75,1)
非常强影响(VH)	4	(0.75,1,1)

令 $x_{ij}^k=(l_{ij}^k,m_{ij}^k,r_{ij}^k)$ 表示第 k 个专家评判得出的第 i 个因素对第 j 个因素的影响度对应的三角模糊数,其中 k = 1,2,……,K。CFCS 方法具体计算过程见公式(2) - 公式(10)。

将三角模糊数标准化:

$$xl_{ij}^k=(l_{ij}^k-\min l_{ij}^k)/\Delta_{\min}^{\max} \quad \text{公式(2)}$$

$$xm_{ij}^k=(m_{ij}^k-\min l_{ij}^k)/\Delta_{\min}^{\max} \quad \text{公式(3)}$$

$$xr_{ij}^k=(r_{ij}^k-\min l_{ij}^k)/\Delta_{\min}^{\max} \quad \text{公式(4)}$$

$$\text{其中 } \Delta_{\min}^{\max}=\max_{1\leqslant k\leqslant K} r_{ij}^k-\min l_{ij}^k \quad \text{公式(5)}$$

计算左标准值(xls)和右标准值(xrs):

$$xls_{ij}^k = xm_{ij}^k/(1 + xm_{ij}^k - xl_{ij}^k) \qquad 公式(6)$$

$$xrs_{ij}^k = xr_{ij}^k/(1 + xr_{ij}^k - xm_{ij}^k) \qquad 公式(7)$$

计算总体清晰值：

$$x_{ij}^k = [xls_{ij}^k(1 - xls_{ij}^k) + xrs_{ij}^k xrs_{ij}^k]/(1 - xls_{ij}^k + xrs_{ij}^k) \qquad 公式(8)$$

$$z_{ij}^k = \min l_{ij}^k + x_{ij}^k \Delta_{\min}^{\max} \qquad 公式(9)$$

计算平均清晰值：

$$z_{ij} = (x_{ij}^1 + z_{ij}^2 + \cdots\cdots + z_{ij}^K)/K \qquad 公式(10)$$

步骤 4：将矩阵 Z 标准化得到直接影响矩阵 H，具体计算过程见公式(11)和公式(12)，其中 q 为标准化系数。

$$q = \frac{1}{\max\limits_{1 \leqslant j \leqslant n} \sum_{j=1}^{n} z_{ij}} \qquad 公式(11)$$

$$H = q * Z \qquad 公式(12)$$

步骤 5：计算综合影响矩阵 T，其中 t_{ij} 表示因素 i 和 j 的间接影响关系，具体计算过程见公式(13)，其中 I 为单位矩阵。

$$T = H(I - H)^{-1} \qquad 公式(13)$$

步骤 6：计算 T 中各个因素的行和(D)及列和(R)，D 为影响度，表示因素对个人云存储服务技术安全风险系统中其他因素直接影响和间接影响的总和，R 为被影响度，表示因素受到个人云存储服务技术安全风险系统中其他因素直接影响和间接影响的总和。$D+R$ 表示因素的中心度，具体是指因素在系统中的重要程度，D-R 表示原因度，将因素划分为原因组(该因素对其他因素的影响大于其自身受到的影响，主动影响其他因素)和结果组(该因素受其他因素的影响程度大，表现为被动影响)，具体计算过程见公式(14)和公式(15)：

$$D = [\sum_{j=1}^{n} t_{ij}]_{n \times 1} \qquad 公式(14)$$

$$R = [\sum_{i=1}^{n} t_{ij}]_{n \times 1} \qquad 公式(15)$$

以上所有公式中 $i, j = 1, 2, \cdots\cdots, n$。

5 关键影响因素识别与分析

关于专家访谈用户规模方面，G. Guest 等[34]指出在访谈调查研究中，调查对象达到 12 人即可视为充分样本。在个人云存储服务领域的研究中，K. Ghaffari 等[35]遴选 12 名用户采用半结构式访谈揭示发展中国家用户使用个人云存储服务现象。因此，借鉴以上研究经验，本文遴选调查对象包括：主持云计算安全领域国家自然科学基金、国家社会科学基金项目负责人及其项目组核心骨干成员 11 名，发表过云计算安全风险评估相关成果作者 3 名、具有 3 年以上使用经验的个人云存储服务资深用户 2 名，最终遴选出 16 位专家或用户进行调查。所有参与调查的对象均具有计算机专业背景，其中具有正高职称 3 人，副高职称 4 人；博士研究生学历 12 人，硕士研究生学历 4 人。

本文通过深入访谈、问卷调查两种方式对个人云存储服务技术安全风险对遴选专家进行调研，笔者课题组 3 名骨干成员针对回收的问卷进行充分讨论和统计分析，根据 Fuzzy-DEMATEL 模型的计算步骤，得出综合影响矩阵 T(见表 4)、中心度 D+R 及原因度 D-R 等指标(见表 5)。根据表 5 数据绘制因果图见图 2。

表 4 个人云存储服务技术安全风险影响因素的综合影响矩阵

代码	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14
F1	0.828	0.900	0.755	0.927	0.916	0.842	0.681	0.880	0.796	0.934	0.816	0.824	0.939	0.804
F2	0.904	0.821	0.755	0.915	0.922	0.840	0.664	0.870	0.791	0.934	0.820	0.820	0.944	0.791
F3	0.801	0.797	0.630	0.837	0.812	0.751	0.617	0.807	0.718	0.827	0.720	0.751	0.838	0.716
F4	0.795	0.794	0.681	0.752	0.795	0.737	0.610	0.788	0.698	0.816	0.721	0.746	0.837	0.726
F5	0.899	0.895	0.752	0.908	0.825	0.833	0.667	0.858	0.781	0.923	0.821	0.814	0.933	0.779
F6	0.901	0.902	0.760	0.926	0.916	0.766	0.672	0.872	0.798	0.936	0.830	0.817	0.944	0.785
F7	0.788	0.784	0.701	0.822	0.793	0.730	0.556	0.808	0.705	0.817	0.730	0.752	0.821	0.720
F8	0.806	0.794	0.696	0.831	0.800	0.736	0.621	0.730	0.703	0.821	0.720	0.755	0.834	0.734
F9	0.858	0.862	0.717	0.867	0.869	0.796	0.652	0.836	0.692	0.888	0.787	0.777	0.893	0.751
F10	0.900	0.893	0.750	0.900	0.905	0.825	0.671	0.865	0.796	0.845	0.822	0.830	0.923	0.780
F11	0.930	0.923	0.792	0.951	0.936	0.860	0.698	0.921	0.810	0.960	0.778	0.863	0.971	0.821
F12	0.757	0.758	0.655	0.791	0.775	0.706	0.589	0.778	0.674	0.804	0.702	0.656	0.808	0.693
F13	0.935	0.924	0.779	0.944	0.938	0.865	0.697	0.916	0.818	0.959	0.847	0.855	0.888	0.831
F14	0.817	0.810	0.698	0.850	0.808	0.740	0.614	0.827	0.709	0.838	0.744	0.765	0.843	0.668

表 5　各因素的影响度、被影响度、中心度和原因度

代码	影响因素	影响度(D)	排序	被影响度(R)	排序	中心度(D+R)	排序	原因度(D-R)	排序
F1	访问控制	11.842	3	11.919	5	23.761	3	-0.077	8
F2	服务/账户劫持	11.791	5	11.857	6	23.649	5	-0.066	7
F3	资源耗尽	10.622	10	10.121	13	20.743	13	0.501	5
F4	数据完整性风险	10.496	13	12.222	3	22.718	8	-1.726	14
F5	加密及密钥管理	11.688	7	12.009	4	23.697	4	-0.321	10
F6	网络安全风险	11.824	4	11.027	8	22.851	7	0.797	3
F7	硬件安全风险	10.526	12	9.010	14	19.536	14	1.516	1
F8	数据备份和恢复	10.583	11	11.756	7	22.339	9	-1.173	13
F9	服务器引擎漏洞	11.245	8	10.491	12	21.736	10	0.754	4
F10	软件安全风险	11.707	6	12.302	2	24.009	2	-0.595	11
F11	虚拟化漏洞	12.217	1	10.858	10	23.075	6	1.358	2
F12	数据移植	10.147	14	11.025	9	21.172	12	-0.878	12
F13	数据传输安全	12.196	2	12.417	1	24.613	1	-0.222	9
F14	数据删除	10.730	9	10.598	11	21.328	11	0.132	6

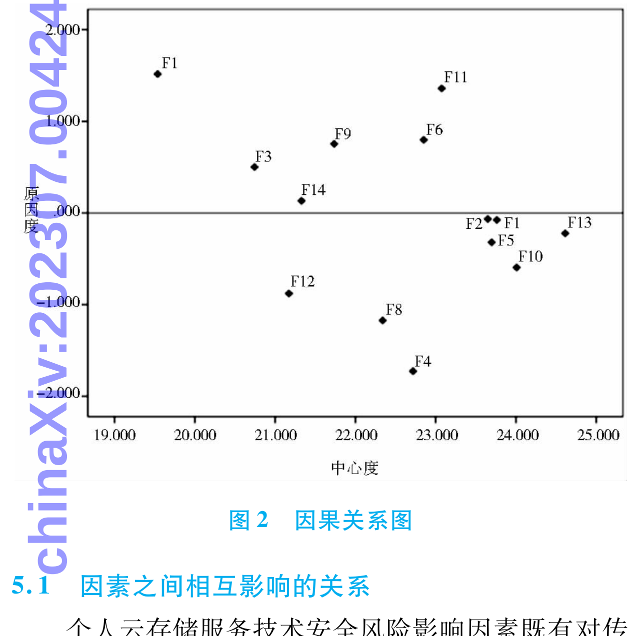


图 2　因果关系图

5.1　因素之间相互影响的关系

个人云存储服务技术安全风险影响因素既有对传统信息技术安全风险的继承性又具有云安全风险特性，个人云存储服务技术安全风险影响因素指标体系所涉及的诸多风险要素相互关联、互相作用，其强度、广度各不相同形成复杂作用机理，在此基础上共同构成了个人云存储安全风险要素复杂系统。

根据各影响因素原因度的正负可将其分为原因组因素和结果组因素。由表 5 和图 2 可知，F3、F6、F7、F9、F11、F14 为原因组因素。虚拟化漏洞 F11 在所有的影响因素中 D 最大，R 得分较低居于第 10 位，表现出强烈的主动性，即表明虚拟化漏洞能够强烈地影响其他因素，但自身却较难受其他因素的影响。例如黑客通过攻击虚拟化漏洞对虚拟机监视器进行控制，攻击位于同一宿主机上的虚拟机窃取用户身份信息，从而导致服务/账户劫持、资源耗尽、用户隐私数据泄露等一系列安全风险[13]。网络安全风险 F6 与 F11 相似，D 排名靠前，R 排名靠后，表现出较强的主动性。资源耗尽 F3、硬件安全风险 F7、服务器引擎漏洞 F9、数据删除 F14 的 D 和 R 得分在所有的因素中均较低，可见这 4 个因素同其他因素之间关系较为疏远。

原因度小于 0 为结果组因素，由表 5 可知，F1、F2、F4、F5、F8、F10、F12、F13 为结果组因素。由图 2 可知，结果组因素的 D + R 普遍高于平均水平，说明这些影响因素重要性突出。结果组因素对个人云存储服务技术安全风险的影响最为直接，也更容易受原因组因素的影响。其中数据传输安全 F13 具有最大的被影响度，但其 D 得分也较高（居于第 2 位），说明 F13 与其他因素之间有很强的联系。F13 最容易受到其他因素的影响，同时对其他因素有较强的影响。F13 被动性要强于主动性，总体仍表现为结果组因素。数据传输过程中可能会存在多种风险从而导致用户数据泄露。数据完整性风险 F4、加密及密钥管理 F5 和软件安全风险 F10 的 R 和 D 排名分别居于第 3 位和第 13 位、第 4 位和第 7 位、第 2 位和第 6 位，表现出较为强烈的被动性。访问控制 F1 和服务/账户劫持 F2 的原因度得分均为负值，但从两个因素的 D 和 R 来看，其 D 排名反而大于 R 排名，这是云计算环境复杂性导致的，且其原因度仅略小于 0，总体上仍表现出一定的被动性。个人云存储用户都有唯一登录身份信息，若信息被泄露，容易导致数据完整性风险、加密密钥丢失、数据非法操作等一系列问题；黑客通过非法获取管理员身份信息可以控制个人云存储系统，引起拒绝服务攻击、服

务/账户劫持等一系列问题。数据备份和恢复 F8 和数据移植 F12 的 D 和 R 均较低,表明 F8、F12 与个人云存储服务的技术安全风险影响因素系统中的其他因素关系较为疏远。

5.2 关键影响因素识别

本文结合 D、R 及 D + R 等指标确定关键影响因素。第一,虚拟化漏洞 F11 在 14 个因素中影响度最大,能够强烈地影响其他 13 个因素的变化,从而确定为关键影响因素。第二,数据传输安全 F13 虽为结果组因素,但其 D 和 R 水平都很高,且其 D + R 排名位于第一,说明该因素在系统中的重要性,与其他因素紧密相连,可见个人云服务提供商在个人云存储建设时,无论是从长期还是短期实施中都应作为关键因素予以考虑,保证数据传输过程的安全,防止非法入侵等。第三,软件安全风险 F10 原因度虽为负值,但其 D 水平也不低(居于第 6 位),说明对其他因素也有一定的影响力,并且其 D + R 水平较高(居于第 2 位)也进一步验证 F10 成为关键因素的结论。第四,访问控制 F1 和服务\账户劫持 F2 的 D -R 得分分别为 -0.077、-0.066(略小于 0),表明 F1 和 F2 受其他因素影响较小,且对个人云存储其他技术安全风险因素有一定的影响。与此同时,两者 D、R 和 D + R 得分均较高,则都可确认为关键因素,该结论进一步支持了 ENISA 提到恶意内部人员可能会带来一系列影响数据或 IP 机密性、完整性和可用性的损害[3]。

资源耗尽 F3、硬件安全风险 F7、服务器引擎漏洞 F9、数据删除 F14、数据备份和恢复 F8 和数据移植 F12 的 D、R 和 D + R 得分均不高,说明 F3、F7、F9、F14、F8、F12 与其他因素之间关系较为疏远,且在系统中的重要性不高。因此,这些因素均为非关键影响因素。数据完整性风险 F4 和加密及密钥管理 F5 表现出较为强烈的被动性,且 D + R 平均不高。通过短期措施对个人云存储的安全提升可起到一定的效果,但由于其易受其他因素影响的特性,在长期建设中不一定有很好的效果,所以不宜作为关键因素考虑。

综上分析讨论可以发现,本文研究结果与 CSA 发布的十二大云安全威胁其中的 10 个技术风险中的身份/登录信息和访问管理不到位、不安全的接口和 APISs、系统安全漏洞、账户劫持、恶意内部人员、共享技术问题、拒绝服务 7 个技术因素是一致的[7]。

6 结论与启示

6.1 结论

影响个人云存储服务技术安全风险的因素较为复杂,各因素之间交叉在一起相互作用,但是不同因素的影响机理和影响程度又不尽相同。已有文献中针对个人云存储服务技术安全风险因素之间相互关系的研究较为鲜见。本文基于文献调研、专家访谈、云计算安全报告(Gartner)、云计算安全架构与标准(ENISA、CSA、FedRAMP、MTCS),提出了 14 个影响个人云存储服务技术安全风险因素,通过 Fuzzy-DEMATEL 方法得出各因素的影响度、被影响度、中心度和原因度指标,根据原因度得分辨析出资源耗尽 F3、网络安全风险 F6、硬件安全风险 F7、服务器引擎漏洞 F9、虚拟化漏洞 F11、数据删除 F14 为原因组因素。访问控制 F1、服务/账户劫持 F2、数据完整性风险 F4、加密及密钥管理 F5、数据备份和恢复 F8、软件安全风险 F10、数据移植 F12、数据传输安全 F13 为结果组因素。综合各项指标分析讨论得出 5 个关键影响因素:虚拟化漏洞 F11、数据传输安全 F13、软件安全风险 F10、访问控制 F1、服务/账户劫持 F2。

6.2 研究意义

理论意义体现在:相对已有研究而言,本研究从传统技术安全风险与云特有技术安全风险两个层面构建了完整的个人云存储服务的技术安全风险评估指标体系,包括 14 个评估指标;揭示了个人云存储服务的技术安全风险影响因素系统中因素之间的因果关系及相对重要程度,分析了个人云存储服务关键技术安全风险因素,研究结论与 CSA 发布的云计算十二大威胁中的技术威胁基本吻合,进一步丰富了个人云存储服务安全风险的理论研究。同时,本研究结果可为个人云存储服务利益相关者在实际开发过程中评估和检验云存储技术安全风险提供理论参考。另外,本研究中构建的个人云存储服务技术安全风险因素可以为云计算的其他领域安全风险评估提供理论借鉴。

实践意义体现在:根据本文的研究结果,个人云存储服务提供商可以在未来进一步从以下方面降低个人云存储服务的技术安全风险,提高用户持续使用的增长率,推进个人云存储服务的安全发展:①进一步完善虚拟化技术。减少个人云存储系统中的磁盘数量,以期降低运营成本、减少资源消耗。同时,虚拟化技术的改进还可以通过延长现有存储设备的使用寿命来降低采购成本,减少为消费者提供个人云存储服务的成本。②进一步加强网络监控技术。个人云存储是基于云计算的新兴存储技术,其数据在网络传输过程中的风险是不可避免的,个人云存储服务提供商可通过采用加强网络入侵检测技术保证传输信道的安全性。通过加

强网络监控,防止黑客注入恶意代码/网络恶意软件,从而确保数据传输通道的安全性。加强网络入侵检测,以发现在个人云存储系统中违反安全策略和被攻击的迹象,从而降低用户数据丢失或泄漏的风险。此外,个人云存储服务提供商应加强与提供网络服务的第三方合作,以提供给用户稳定且充足的带宽资源。③对不同类型端点对应的接口进行校验,并采用安全套接层(SSL)进行防护;不断完善云存储软件,查找软件自身存在的漏洞并修正,对软件日志、补丁不断修复,保障软件更新升级之后不会出现服务中断或数据不兼容等问题。④完善用户身份认证技术和授权技术,能够有效地控制非法用户通过窃取授权用户身份信息对用户数据进行不正当操纵的风险,在一定程度上也能减少服务劫持安全事件的发生。

6.3 创新与不足

本研究主要创新之处在于:构建了一套科学、完整的用于评估个人云存储服务技术安全风险指标体系,揭示了个人云存储服务的技术安全风险因素系统中关键因素及其相互之间的因果关系。研究局限表现在:本研究采用的是小样本调查,未来的研究可以通过扩大调查专家的样本规模和范围,如调查个人云存储服务行业从业人员,以检验研究结论的稳健性。

本文仅从技术安全层面对个人云存储服务安全风险关键影响因素进行了识别与分析,下一步将从管理,政策与法律法规维度对个人云存储服务安全风险进行讨论,以期实现个人云存储服务安全风险三位一体评估目标,丰富云计算安全的理论研究,为个人云存储服务可持续发展提供更全面的实践建议。

参考文献:

[1] HASHIZUME K, ROSADO D G, FERNÁNDEZ-MEDINA E, et al. An analysis of security issues for cloud computing [J]. Journal of internet services & applications,2013,4(1):1－13.

[2] 艾媒咨询. 2016 年中国个人云盘行业研究报告[EB/OL]. [2018－07－05]. http://www.iimedia.cn/45865.html.

[3] ENISA. Cloud computing benefits, risks and recommendations for information security: cloud computing security risk assessment [EB/OL]. [2018－07－17]. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

[4] ZISSIS D, LEKKAS D. Addressing cloud computing security issues [J]. Future generation computer systems,2012,28(3):583－592.

[5] SINGH A, CHATTERJEE K. Cloud security issues and challenges: a survey [J]. Journal of network & computer applications, 2017,79(2):88－115.

[6] Gartner Group. Assessing the security risks of cloud computing [EB/OL]. [2018－07－17]. https://s3.amazonaws.com/academia.edu.documents/33355553/Gartner_Security_Risks_of_Cloud.pdf? AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1531800717&Signature=9iWiV8np8Hv%2BSVw5cvl8sRGqzVw%3D&response-content-disposition=inline%3B%20filename%3DAssessing_the_Security_Risks_of_Cloud_Co.pdf.

[7] CSA. 'The treacherous twelve' cloud computing top threats in 2016 [EB/OL]. [2018－07－05]. https://www.prnewswire.com/news-releases/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016-300227806.html.

[8] KHAN N, AL-YASIRI A. Identifying cloud security threats to strengthen cloud computing adoption framework [J]. Procedia computer science,2016,94:485－490.

[9] RAMACHANDRA G, IFTIKHAR M, KHAN F A. A comprehensive survey on security in cloud computing [J]. Procedia computer science,2017,110:465－472.

[10] SHAMELI-SENDI A, CHERIET M. Cloud computing: a risk assessment model [C]//IEEE International Conference on Cloud Engineering. Washington: IEEE, 2014:147－152.

[11] LIU J, GUO Z. Research on cloud security risk assessment based on fuzzy entropy weight model [J]. Electrics, electronics, and computer science,2016,139:390－395.

[12] LIN G T R, LIN C C, CHOU C J, et al. Fuzzy modeling for information security management issues in cloud computing [J]. International journal of fuzzy systems,2014,16(4):529－540.

[13] LIN F, ZENG W, YANG L, et al. Cloud computing system risk estimation and service selection approach based on cloud focus theory [J]. Neural computing and applications,2017,28(1):1863－1876.

[14] ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services [EB/OL]. [2018－07－17]. https://www.iso.org/standard/43757.html.

[15] BSI Group. ISO/IEC 27017, Extending ISO/IEC 27001 into the Cloud [EB/OL]. [2018－07－17]. https://www.bsigroup.com/LocalFiles/EN-AU/_Brochures/ISO%2027017%20Whitepaper-JULY2016.pdf.

[16] FedRAMP. Security assessment framework [EB/OL]. [2018－07－17]. https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/01/FedRAMP-Security-Assessment-Framework-v2-1.pdf.

[17] Singapore MTCS. SS584 (2016), Specification for multi-tiered cloud computing security [EB/OL]. [2018－07－17]. https://www.singaporestandardseshop.sg/Product/Product.aspx? id = 88be024c-cead-4a59-801d-9fcedbbab88f.

[18] CSA. Security guidance for critical areas of focus in cloud computingV2.1 [EB/OL]. [2018－07－17]. https://www.rationalsurvivability.com/blog/2009/12/cloud-security-alliance-v2-1-security-guidance-for-critical-areas-of-focus-in-cloud-computing-available/.

[19] ENISA. A guide to monitoring of security level in cloud contracts [EB/OL]. [2018－07－17]. https://www.enisa.europa.eu/

publications/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts.
[20] SHAHZAD F. State-of-the-art survey on cloud computing security challenges, approaches and solutions [J]. Procedia computer science, 2014, 37: 357 – 362.
[21] SHIRVANI M H, RAHMANI A M, SAHAFI A. An iterative mathematical decision model for cloud migration: a cost and security risk approach [J]. Software practice & experience, 2018, 48(6): 449 – 485.
[22] MACKAY M, BAKER T, AL-YASIRI A. Security-oriented cloud computing platform for critical infrastructures [J]. Computer law & security review the international journal of technology & practice, 2012, 28(6): 679 – 686.
[23] KANG W M, DONG-LEE J, JEONG Y S, et al. VCC-SSF: service-oriented security framework for vehicular cloud computing [J]. Sustainability, 2015, 7(2): 2028 – 2044.
[24] WALTERBUSCH M, FIETZ A, TEUTEBERG F. Missing cloud security awareness: investigating risk exposure in shadow IT [J]. Journal of enterprise information management, 2017, 30(4): 644 – 665.
[25] 姜茸,杨明,马自飞,等. 云计算安全风险度量评估与管理[M]. 北京:科学出版社,2016.
[26] COPPOLINO L, D'ANTONIO S, MAZZEO G, et al. Cloud security: emerging threats and current solutions [J]. Computers & electrical engineering, 2017, 59: 126 – 140.
[27] CHOI M, LEE C. Information security management as a bridge in cloud systems from private to public organizations [J]. Sustainability, 2015, 7(9): 12032 – 12051.
[28] SINGH S, JEONG Y S, PARK J H. A survey on cloud computing security: issues, threats, and solutions [J]. Journal of network & computer applications, 2016, 75(9): 200 – 222.
[29] 阮树骅,瓮俊昊,毛麾,等. 云安全风险评估度量模型[J]. 山东大学学报:理学版,2018,53(3):71 – 76.
[30] RONG C, NGUYEN S T, JAATUN M G. Beyond lightning: a survey on security challenges in cloud computing [J]. Computers & electrical engineering, 2013, 39(1): 47 – 54.
[31] BRENDER N, MARKOV I. Risk perception and risk management in cloud computing: results from a case study of Swiss companies [J]. International journal of information management, 2013, 33(5): 726 – 733.
[32] LIN R J. Using fuzzy dematel to evaluate the green supply chain management practice [J]. Journal of cleaner production, 2013, 40(7): 32 – 39.
[33] OPRICOVIC S, TZENG G H. Defuzzification within a multi-criteria decision model [J]. Uncertain fuzzy, 2003, 11(5): 635 – 652.
[34] GUEST G, BUNCE A, JOHNSON L. How many interviews are enough?: an experiment with data saturation and variability [J]. Field methods, 2006, 18(18): 59 – 82.
[35] GHAFFARI K, LAGZIAN M. Exploring users' experiences of using personal cloud storage services: a phenomenological study [J]. Behaviour & information technology, 2018, 37(3): 295 – 309.

作者贡献说明:
程慧平:提出文章选题及核心思路,修改论文;
彭琦:撰写和修改论文初稿。

Identification and Analysis of the Key Influencing Factors on Technical Security Risk of Personal Cloud Storage Service

Cheng Huiping[1,2] Peng Qi[2]
[1] School of Economics and Management of Hubei University of Technology, Wuhan 430068
[2] School of Public Management of Northwest University, Xi'an 710127

Abstract: [**Purpose/significance**] In recent years, the technical security problems of personal cloud storage service are common, which severely hinders users' continuous usage of personal cloud storage service. It is of great practical significance to identify and analyze the key factors that affect the technical security risk of personal cloud storage service for personal cloud storage service providers to offer secure cloud storage service as well as increase user engagement with personal cloud storage service. [**Method/process**] Based on literature surveys, expert interviews, cloud computing security reports put forward by Gartner, and cloud computing security frameworks and standards (ENISA, CSA, FedRAMP, MTCS), the technical security risk factors indicator system of personal cloud storage service is constructed. The direct influence matrix between the influencing factors of technical security risk evaluation indicator system of personal cloud storage service is obtained through questionnaire survey with experts. This paper analyzes the causal category and the degree of importance of the influencing factors of personal cloud storage service technical security risks by applying Fuzzy-DEMATEL method, and identifies the key influencing factors of personal cloud storage service technical security risk. [**Result/conclusion**] The critical influencing factors of personal cloud storage service technical security risk are: access control,

service / account hijacking, software security risk, virtualization vulnerability, and data transmission security. Finally, according to the empirical conclusions, it provides feasible technical advice for building a secure cloud storage service for personal cloud storage service providers. This study enriches the theoretical research results of personal cloud storage service security risk, and provides practical references for the personal cloud storage service providers to guarantee user data security.

Keywords: personal cloud storage service　cloud storage security　cloud computing security　Fuzzy-DEMATEL　technical security risk

《知识管理论坛》投稿须知

《知识管理论坛》(CN11 - 6036/C,ISSN 2095 - 5472)是由中国科学院文献情报中心主办的网络开放获取学术期刊,2017 年入选国际著名的开放获取期刊名录(DOAJ)。《知识管理论坛》致力于推动知识时代知识的创造、组织和有效利用,促进知识管理研究成果的快速、广泛和有效传播。

1. 报道范围

稿件的主题应与知识相关,探讨有关知识管理、知识服务、知识创新等相关问题。稿件可侧重于理论,也可侧重于应用、技术、方法、模型、最佳实践等。

2. 学术道德要求

投稿必须为未公开发表的原创性研究论文,选题与内容具有一定的创新性。引用他人成果,请务必按《著作权法》有关规定指明原作者姓名、作品名称及其来源,在文后参考文献中列出。

本刊使用 CNKI 科技期刊学术不端文献检测系统(AMLC)对来稿进行论文相似度检测,如果稿件存在学术不端行为,一经发现概不录用;若论文在发表后被发现有学术不端行为,我们会对其进行撤稿处理,涉嫌学术不端行为的稿件作者将进入我刊黑名单。

3. 署名与版权问题

作者应该是论文的创意者、实践者或撰稿者,即论文的责任者与著作权拥有者。署名作者的人数和顺序由作者自定,作者文责自负。所有作者要对所提交的稿件进行最后确认。

论文应列出所有作者的姓名,对研究工作做出贡献但不符合作者要求的人要在致谢中列出。

论文同意在我刊发表,以编辑部收到作者签字的"论文版权转让协议"为依据。

依照《著作权法》规定,论文发表前编辑部进行文字性加工、修改、删节,必要时可以进行内容的修改,如作者不同意论文的上述处理,需在投稿时声明。

我刊采用知识共享署名(CC BY)协议,允许所有人下载、再利用、复制、改编、传播所发表的文章,引用时请注明作者和文章出处(推荐引用格式如:吴庆海. 企业知识萃取理论与实践研究[J/OL]. 知识管理论坛, 2016, 1(4): 243 - 250[引用日期]. http://www.kmf.ac.cn/p/1/36/.)。

4. 写作规范

本刊严格执行国家有关标准和规范,投稿请按现行的国家标准及规范撰写;单位采用国际单位制,用相应的规范符号表示。

5. 评审程序

执行严格的三审制,即初审、复审(双盲同行评议)、终审。

6. 发布渠道与形式

稿件主要通过网络发表,如我刊的网站(www.kmf.ac.cn)和我刊授权的数据库。

本刊已授权数据库有中国期刊全文数据库(CNKI)、龙源期刊网、超星期刊域出版平台等,作者稿件一经录用,将同时被该数据库收录,如作者不同意收录,请在投稿时提出声明。

7. 费用

自 2016 年 1 月 1 日起,在《知识管理论坛》上发表论文,将免收稿件处理费。

8. 关于开放获取

本刊发表的所有研究论文,其出版版本的 PDF 均须通过本刊网站(www.kmf.ac.cn)在发表后立即实施开放获取,鼓励自存储,基本许可方式为 CC - BY(署名)。详情参阅期刊首页 OA 声明。

9. 选题范围

互联网与知识管理、大数据与知识计算、数据监护与知识组织、实践社区与知识运营、内容管理与知识共享、数据关联与知识图谱、开放创新与知识创造、数据挖掘与知识发现。

10. 关于数据集出版

为方便学术论文数据的管理、共享、存储和重用,近日我们通过中国科学院网络中心的 ScienceDB 平台(www.sciencedb.cn)开通数据出版服务,该平台支持任意格式的数据集提交,欢迎各位作者在投稿的同时提交与论文相关的数据集(稿件提交的第 5 步即进入提交数据集流程)。

11. 投稿途径

本刊唯一投稿途径:登录 www.kmf.ac.cn,点击作者投稿系统,根据提示进行操作即可。